IN THE CLAIMS:

The following is a current listing of claims and will replace all prior versions and listings of claims in the application. Please amend the claims as follows:

1. (Currently Amended) A method performed by an information handling system, the method comprising:

making a determination of the likelihood that a first web page ~~resource~~ received from a first computer network is misrepresented as being from a trusted source, including determining that the first web page includes content associated with a request for a financial account number of a user of the information handling system ~~coupled to the first computer network~~.

2. (Canceled)

3. (Currently Amended) The method of claim 1 [[2]], wherein the content is an information entry field embedded in the first web page.

4. (Currently Amended) The method of claim 1 [[2]], wherein ~~the web page is a first web page, and wherein~~ the content is an address of a second web page.

5. (Original) The method of claim 4, wherein the address is a hyperlink embedded in the first web page.

6-17. (Canceled)

18. (Currently Amended) The method of claim 1[[7]], wherein the financial account number ~~information~~ is for ~~information about~~ a bank account of the user.

19. (Currently Amended) The method of claim 1[[7]], wherein the financial account number ~~information~~ is for ~~information about~~ a credit card account of the user.

20-30. (Canceled)

31. (Currently Amended) A system, comprising:

~~one or more processors;~~

a computer configured to execute program instructions;

memory storing program instructions executable by the computer ~~one or more processors~~ to:

make a determination that a first web page ~~resource~~ received from a first computer network is misrepresented as being from a trusted source, including determining that the first web page includes content associated with a request for a financial account number of a user of the system. ~~coupled to the first computer network;~~

32. (Canceled)

33. (Currently Amended) The system of claim 31 [[32]], wherein the content is an information entry field embedded in the first web page.

34. (Currently Amended) The system of claim 31 [[32]], wherein the ~~web page is a first web page, and wherein the~~ content is an address of a second web page.

35. (Original) The system of claim 34, wherein the address is a hyperlink embedded in the first web page.

36-47. (Canceled)

48. (Currently Amended) The system of claim 31 [[47]], wherein the financial account number ~~information~~ is for ~~information about~~ a bank account of the user.

49. (Currently Amended) The system of claim 31 [[47]], wherein the financial account number ~~information~~ is for ~~information about~~ a credit card account of the user.

50-60. (Canceled)

61. (Currently Amended) A tangible computer-readable memory medium storing program instructions that are executable by a computing device to:

make a determination that a first web page ~~resource~~ received from a first computer network is misrepresented as being from a trusted source, including by determining that the first web page includes content requesting a financial account number of a user of the computing device ~~coupled to the first computer network~~.

62. (Canceled)

63. (Currently Amended) The tangible computer-readable memory medium of claim 61 [[62]], wherein the content is an information entry field embedded in the first web page.

64-77. (Canceled)

78. (Currently Amended) The tangible computer-readable memory medium of claim 61 [[77]], wherein the financial account number ~~information~~ is for ~~information about~~ a bank account of the user.

79. (Currently Amended) The tangible computer-readable memory medium of claim 61 [[77]], wherein the financial account number ~~information~~ is for ~~information about~~ a credit card account of the user.

80-127. (Canceled)

128. (Currently Amended) The method of claim 1, wherein said determination further includes a determination ~~is~~ whether the first web page ~~resource~~ is from a trusted source, an untrusted source, or a source that cannot be identified as a trusted or untrusted ~~whether the~~ source ~~of the first resource is undetermined~~.

129. (Currently Amended) A tangible computer-readable memory medium storing program instructions that are executable on an information handling system to:

categorize a web page ~~data~~ received via an external network interface of the information handling system as ~~to the likelihood of the received data~~ spoofing its origin, not spoofing its origin, or indeterminate as to whether the received web page is spoofing its origin.

130-133. (Canceled)

134. (Currently Amended) A tangible computer-readable memory medium storing program instructions that are executable on an information handling system to:

receive data from an external network coupled to the information handling system;

analyze the received data to make a determination whether the received data indicates that it is from a first source coupled to the external network, but is actually from a second source coupled to the external network; and

wherein the determination is based, at least in part, on an age of the received data, and/or a size of the received data.

135. (Currently Amended) The tangible computer-readable memory medium of claim 134, wherein the received data includes information indicating that it is from a source trusted by a user of the information handling system.

136. (Currently Amended) The tangible computer-readable memory medium of claim 135, wherein the received data is intended to cause the user to supply confidential information to a source other than the trusted source.

137. (Currently Amended) The tangible computer-readable memory medium of claim 136, wherein the confidential information is financial information of the user.

138. (Currently Amended) The tangible computer-readable memory medium of claim 136, wherein the confidential information is login information of the user.

139. (Currently Amended) A method, comprising:

receiving ~~data~~ a web page at a first computing device via a wide-area network, wherein the ~~data~~ web page includes information indicating that ~~the~~ its origin ~~of the received data~~ is a first source that is ~~known and~~ trusted by a user of the first computing device;

sending data to the web page that is requested by the web page; and

analyzing the origin's response ~~the received data~~ to the sent data to determine whether the origin of the received ~~data~~ web page is the first source.

140-141. (Canceled)

142. (Currently Amended) The method of claim 139, wherein the web page ~~received data~~ solicits confidential information from the user ~~of the first computing device~~.

143-152. (Canceled)

153. (New) A method, comprising:

making a determination of the likelihood that a web page received from a first computer network is misrepresented as being from a trusted source, including:

analyzing a layout of the web page; and

determining that the layout of the web page is similar to a layout of a known mistrusted web page.

154. (New) The method of claim 153, wherein said making said determination further includes determining whether the web page's markup language contains the trusted source's name or logo and whether the web page has the same organization of content as the trusted source.

155. (New) A method, comprising:

making a determination of the likelihood that a web page received from a first computer network is misrepresented as being from a trusted source, wherein the determination is based on one or more of the following criteria: an age of the web page, a size of the web page, a number of hyperlinks to the web page from trusted sources.

156. (New) The method of claim 155, wherein the determination is based, at least in part, on the age of the web page and the size of the web page.

157. (New) The method of claim 155, wherein the determination is based, at least in part, on the age of the web page and the number of hyperlinks to the web page from trusted sources.

158. (New) A tangible computer-readable memory medium storing program instructions that are executable on a computing device to:

make a determination of the likelihood that a web page received from a first computer network is misrepresented as being from a trusted source coupled to the first computer network, including:

analyzing a layout of the web page; and

determining that the layout of the web page is similar to a layout of a known mistrusted web page.

159. (New) A tangible computer-readable memory medium storing program instructions that are executable on a computing device to:

make a determination of the likelihood that a web page received at the computing device from a first computer network is misrepresented as being from a trusted source, wherein the determination is based on one or more of the following criteria: an age of the web page, a size of the web page, a number of hyperlinks to the web page from known trusted sources.